according to the principles of control engineering. Additionally, the topology model **46** reveals a value for the down time T.

[0061] The reachability analysis can ascertain the state trajectory for different operating points of the operating range B in a step S**10** and, in a step S**12**, can check a safety criterion **48** for each state trajectory, that is to say whether the respective state trajectory reaches the set V, for example. If this is the case, symbolized by a plus sign (+) in FIG. **4**, then a safety measure is initiated in a step **48**, such as the described display of the critical operating point by the engineering system E, for example. Otherwise, that is to say if all state trajectories signal a safe changeover action (symbolized by a minus sign (−) in FIG. **4**), the failure tolerance of the topology model **46**, that is to say of the automation installation **10** in its present design state, can be signaled in a step S**16**.

[0062] Hence, the exemplary embodiment as a whole describes a method for model-based determination of the effects of a failover in a high-availability automation system on a process that is to be controlled.

LIST OF REFERENCE SYMBOLS

[0063] **10** Automation installation
[0064] Process
[0065] **14**, **16** Peripheral component
[0066] **18** Communication network
[0067] **20**, **22** Control apparatus
[0068] **24** Synchronization connection
[0069] **26** Control connection
[0070] **28** Decoupled control connection
[0071] **30** Controlled system model
[0072] **32** Controlled system
[0073] **34** Observer
[0074] **36**, **38** Subtraction point
[0075] **40** Integrator
[0076] **42** Reachability analysis
[0077] **44** Process model
[0078] **46** Topology model
[0079] **48** Safety criterion
[0080] E Engineering system
[0081] U, U' Control output
[0082] R, R' Control system
[0083] W Nominal value preset
[0084] T Down time
[0085] S**10**-S**16** Method step
[0086] Ustat Steady control output

1.-**15**. (canceled)

16. A method for monitoring a failure tolerance for an automation installation, comprising:

providing a controlled system and at least two control apparatuses, said at least two control apparatus alternately controlling the controlled system during a normal operation by outputting control outputs, said automation installation operating a process via the control system;

prompting a changeover between the at least two apparatuses at a failure;

continuously operating the controlled system during the changeover in a controller-less operation for a down time;

ascertaining a possible operating point for the controlled system during the normal operation;

simulating a controller-less operation for each operating point for a duration of the down time to thereby ascertain a state trajectory starting out from the operating point for the controlled system;

checking whether the state trajectory fails to meet a predetermined safety criterion; and if affirmative initiating a predetermined protective measure to avoid the at least operating point.

17. The method of claim **16**, wherein the controller-less operation is simulated by a simulation starting out from the at least one operating point using a model of the controlled system by temporally and successively computing the at least one operating point and the at least one computed operating point is combined to produce the state trajectory.

18. The method of claim **16**, wherein the safety criterion includes whether the state trajectory comprises the at least one operating point that lies outside a predetermined admissible operating range, and/or whether a dynamic transition between two operating points of the state trajectory is greater than a predetermined maximum admissible dynamic range.

19. The method of claim **16**, wherein a protective measure comprises outputting a warning to a user of the automation installation.

20. The method of claim **19**, wherein during the controller-less operation a constant control output is transmitted to the controlled system and the protective measure comprising the constant control output is ascertained that reveals for a respective operating point a safe trajectory for continued operation of the controlled system and the ascertained constant control output is assigned to the at least one operating point.

21. The method of claim **20**, wherein the respective operating point is assigned a safety control output that is output at the operating point in an event of the changeover and interrupts an operation of the controlled system.

22. The method of claim **19**, wherein the protective measure comprises engineering data from the automation installation being taken as a basis for ascertaining an installation component causing the greatest proportion of the down time, and/or adopting an inadmissible operating point in line with the state trajectory.

23. The method of claim **19**, wherein the control apparatuses use a synchronization connection to interchange synchronization data for aligning controller states and the protective measure comprises a rate of the synchronization connection being increased.

24. The method of claim **20**, wherein the protective measure comprises the respective operating point being excluded from the normal operation and controller parameters of the control apparatuses being adjusted.

25. The method of claim **17**, wherein the simulation includes an assumption about a maximum absolute value of a disturbance variable acting in the controlled system for the simulation and the protective measure includes the maximum absolute value being decreased and a new simulation being performed and the disturbance variable being indicated if the safety criterion is met for the new simulation.

26. The method of claim **19**, wherein a new monitoring of the failure tolerance is iteratively performed after the protective measure is performed.